Kathryn Diemer
Diemer, Whitman & Cardosi, LLP
75 East Santa Clara Street, Suite 290
San Jose, CA 95113
Phone: 408-971-6270
Fax: 408-971-6271
kdiemer@diemerwhitman.com
CA Bar No.: 133977

Frank Jablonski (*Pro Hac Vice*)
Progressive Law Group LLC
354 West Main Street
Madison, WI 53703
Phone 608-258-8511
Fax: 608-442-9494
frankj@progressivelaw.com

Elizabeth Roberson-Young (*Pro Hac Vice*)
Mark Bulgarelli (*Pro Hac Vice*)
Progressive Law Group LLC
1 N. LaSalle Street, Suite 2255
Chicago, IL 60602
Tel: 312-787-2717
Fax: 888-574-9038
liza@progressivelaw.com
markb@progressivelaw.com

Counsel for Plaintiff Alice C. Svenson

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

Alice Svenson, individually and on behalf of all others similarly situated, Plaintiff, v. Google, Inc., a Delaware Corporation, and Google Payment Corporation, a Delaware Corporation, Defendants.	Case No. 13-cv-04080-BLF CLASS ACTION PLAINTIFF'S RESPONSE TO DEFENDANTS' MOTION TO DISMISS COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT Date: January 15, 2015 Time: 9:00 a.m. Courtroom 3, 5th Floor Judge: Hon. Beth Labson Freeman

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

STATE CASES

STATUTES

RULES

LEGISLATIVE MATERIALS

INTRODUCTION

The only relevant facts on a motion to dismiss are the pleaded facts and appended documents. Defendants' Motion depends on denying facts in both.

In their second effort to dismiss Plaintiff's claims, Defendants recycle their old arguments against the new facts described in the First Amended Complaint, which depicts Defendants' general strategy of extracting profit from Wallet transactions while evading responsibility for Wallet's mistakes. These contentions, however, no longer apply. The FAC remedies the concerns this Court voiced in its first review of Plaintiff's claims. Defendants' remaining arguments boil down to mere disagreement with Plaintiff's account of the facts. But these factual issues preclude dismissal of Plaintiff's claims and require the Court to deny Defendants' Motion.

The FAC makes it plain that Plaintiff paid Defendants money as part of her Wallet transaction, from which Defendants kept 30% of the purchase price. Defendants concede a contract exists, but they deny that Plaintiff provided any consideration. They cannot have it both ways: a contract requires mutual consideration, which can be valued. Here, that consideration includes both personal information about Plaintiff, which has market value, and Plaintiff's payment of money to Defendants. Under Defendants' contract terms, Plaintiff's personal information was to be kept private. Defendants nonetheless passed it forward into a recognized marketplace, depriving Plaintiff of the value of her information and keeping part of her App payment for themselves. These are breaches with concrete economic injury establishing standing and damages for her state-law claims.

Moreover, the information Defendants passed forward was organized in electronic "packets." This includes personal information, creditworthiness, and buying interest, and is the "content" needed to process the transaction. By disclosing this "content," Defendants also violated the Stored Communications Act.

Defendants muster no additional arguments against the FAC's new allegations. Their

Motion should be denied.[1]

STATEMENT OF RELEVANT FACTS

Defendants provide an online digital content store ("Google Play") and a payment-processing service ("Google Wallet," or "Wallet"). Consumers who buy content offered for sale on Google Play must use Wallet. FAC, ¶¶ 26, 32. Use of Wallet is governed by three interrelated contracts: the Google Wallet Terms of Service ("GWToS"), the "Google Wallet Privacy Policy," or "GWPP," and the Google Privacy Policy ("GPP"), collectively the "Wallet Terms." *Id.,* ¶¶ 33, 54; Exs. A, B, C.

The Wallet Terms explicitly distinguish a "Customer" (a person who merely registers for the Wallet service), from a "Buyer" (who makes a purchase for money). *Id.*, ¶¶ 36, 54; Ex. A at 2. Indeed, at least six of the twelve sections of the Terms that govern purchase transactions (the "Wallet Processing Service") *only* apply to "Buyers." *Id.,* ¶ 37; Ex. A. A Customer only becomes a Buyer by entering a new contract at the time of purchase. None of the contractual rights or obligations arising because of purchase transactions are operative until and unless a consumer, regardless whether she is already a Customer, enters the new and separate contract for each purchase. Defendants impose this requirement and allow no alternative.

The provisions of the Wallet Terms applicable to Buyers (the "Buyer Contract") entail a distinct set of rights and obligations.[2] FAC, ¶¶ 38-40. A key one, for this case, is that Defendants are only authorized to "share ... personal information with other companies outside of Google ...

---

[1] Should the Court grant any part of the motion to dismiss, any shortcomings can be cured by amendment and Plaintiff respectfully requests leave to amend. Even in cases where dismissal is granted, "a district court should grant leave to amend ... unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Doe v. United States*, 58 F.3d 494, 497 (9th Cir. 1995) (citations omitted).

[2] Defendants contend that the FAC invents a new, "fictional" Buyer Contract, *see* Dkt. 89 at 12, but that term is really just meant to clarify the specific rights and obligations imposed on different users by the Wallet Terms, which the FAC plainly identifies as the relevant contract. For instance, the provisions of the Terms that govern purchase, payment, and credit-card processing do not apply to users who merely download free Apps and do not pay for anything. *See, e.g.*, FAC, ¶¶ 36-40, 43-46. The terms "Buyer Contract" and "Customer Contract" are simply useful shorthand for distinguishing between the contract terms that govern paid transactions vs. free downloads, and are not intended to purport that any additional contracts are in play aside from the three agreements expressly identified and attached as exhibits. See FAC, Exs. A, B, C.

[a]s necessary to process your transaction and maintain your account." Ex. B at 2; FAC, ¶¶ 12, 54. This obligation exists only in a Buyer Contract because only a Buyer Contract involves a "transaction." Only a Wallet transaction – that is, the Buyer's purchase transaction pursuant to the separate contract Defendants require – creates the potential for disclosure to a third party, such as an App vendor. *Id.,* ¶ 55; Ex. B. Absent a user's purchase via Wallet, this obligation, and every other obligation Defendants owe to Buyers, is nonexistent.[3] *Id.*, ¶¶ 121; Exs. A and B.

Defendants require that a Buyer agree to a new Buyer Contract each time she makes a purchase. FAC, ¶¶ 2, 34, 35, 60. Without forming that purchase-specific contract, which requires a Buyer to accede to the then-current Wallet Terms, a purchase transaction is impossible. This is true whether or not a user had already agreed to the same terms when registering, whether she had previously agreed to the same terms when making an earlier purchase, or whether she had never previously registered for Wallet, which is Plaintiff Svenson's situation.[4] *Id.*, ¶¶ 38, 43, 60, 88.

When a Buyer purchases content from Google Play, she pays the purchase price to Defendants, who take a 30% cut for themselves before passing the remainder on to the App Vendor. FAC, ¶¶ 4, 46-49, 71, 114, 117. Financial receipts and credit-card statements from Wallet purchases show Defendants to be identified parties to the transaction.[5] *Id.*, ¶ 91-92; Ex. D. Defendants are the first to receive the monies paid by Buyers, are the only entities that ever possess all of the money paid, and collect their 30% fee up front. Defendants hold the remaining 70% until the App Vendor has met additional conditions beyond the App purchase itself (such as reaching a certain dollar threshold in the Vendor's account) and thus also receive the time value of money from the Buyer's payment.[6] *Id.*, ¶¶ 92, 114; Ex. D.

---

[3] Defendants dispute these allegations. *See* Dkt. 89 at 3-4; FAC Ex. A, § 3-5. However, as the Terms are written, the information a consumer must provide to become a Customer is not sufficient to make that consumer a Buyer. FAC, ¶¶ 36-44.

[4] Defendants dispute these allegations. *See* Dkt. 89 at 4.

[5] Defendants dispute this allegation. *See* Dkt. 89 at 4; *but see* Ex. D (showing Defendants listed on Plaintiff's credit card statement documenting her Wallet transaction).

[6] Even presuming Buyers were required to only pay a putatively pure "Vendor's fee," as asserted by Defendants – and this is contested – the payment still represents consideration. Requiring Buyers to pay the fee in order to secure a desired App enhances Defendants' control, ensures they are paid, and paid first, avoids for them potential collection costs that would otherwise arise with their far-flung Vendor network, and channels to Defendants the time value of collected money.

When a Buyer clicks a software button consummating her purchase, she simultaneously agrees to the Buyer Contract and authorizes the transaction. This triggers creation of digital information specific to that purchase, including digital authorization for the purchase, digital identification of the content being purchased, and specific, one-time digital confirmation that the Buyer has just accepted the Wallet Terms currently in effect. *Id.*, ¶¶ 60-64, 88-89. This digital information, commonly sent in electronic "Packets," may also direct additional stored or just-entered data to be placed into the Packets associated with the purchase transaction. All this functional data is distinct from routing data (source and destination) and other data that users' mobile devices and Defendants' servers use to administer the Packets so they go to the right place and arrive in the right form. *Id.*, ¶¶ 5, 63.

In other words, when a Buyer executes the contract required by each purchase of digital content from Google Play via Google Wallet, she clicks a single button that authorizes payment to Defendants and signifies her agreement to new privacy and other obligations associated with her purchase. FAC, ¶¶ 61-62; Exs. A and B. Even though these privacy obligations are triggered only in connection with payment, Defendants nevertheless disclose some of the Buyer's information ("Packet Contents," including her identity, address, city, zip code, email address, or telephone number) to the App Vendor who developed the purchased App. FAC, ¶ 71. This is a breach. The Wallet privacy terms, which become operative only with execution of a Buyer Contract, expressly prohibit this type of disclosure. *Id.,* ¶¶ 71-74. At no point do Defendants inform Buyers of the disclosures, nor do Buyers authorize or consent to this activity. *Id.,* ¶¶ 77-79.

One result of Defendants' actions is that the value of Buyer Contracts – which trigger Defendants' enforceable privacy and data handling obligations – is diminished, as those obligations are breached immediately upon Buyers' purchases. FAC, ¶ 123. Defendants' actions also diminish Buyers' ability to exploit, on their own terms, their personal information in the vast data marketplace around which Defendants have built their multi-billion dollar business. *Id*., ¶¶ 97-103. Defendants' denial of the full benefit of the Buyer Contract, as well as their unauthorized disclosures to third parties of the substance of Buyers' electronic communications, are unlawful.

Id., ¶¶ 123, 216. Indeed, Defendants' practices, as described in the FAC, have drawn both Congressional scrutiny and critical attention from consumers. *Id.*, ¶¶ 81-83. Defendants ceased their practice of disclosing the contents of Buyers' transaction communications shortly after Plaintiff filed her original complaint. *Id.*, ¶ 11.

GOVERNING LEGAL STANDARDS

I. Federal Rule of Civil Procedure 12(b)(1).

The Court evaluates a motion to dismiss for lack of Article III standing under Rule 12(b)(1). *See White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). In deciding a Rule 12(b)(1) motion, "a district court must accept as true all material allegations in the complaint, and must construe the complaint in the nonmovant's favor." *Bernhardt v. County of Los Angeles*, 279 F.3d 862, 867 (9th Cir. 2002). Plaintiffs need only plead general factual allegations to survive a motion to dismiss because the Court will "presume that general allegations embrace those specific facts that are necessary to support the claim." *LSO, Ltd. v. Stroh*, 205 F.3d 1146, 1156 (9th Cir. 2000) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)). Further, the Court may not speculate as to the plausibility of the plaintiff's allegations. *Bernhardt*, 279 F.3d at 867.

II. Federal Rule of Civil Procedure 12(b)(6)

The Federal Rules of Civil Procedure require only that a complaint contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. Pro. 8(a)(2). A complaint need simply state "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotations omitted). The Court "must take allegations as true no matter how skeptical [it] may be." *Iqbal*, 556 U.S. at 696; *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007). A claim is facially plausible and should not be dismissed if its pleaded facts "allow the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Sonoma County Ass'n of Retired Emples. v. Sonoma County*, 708 F.3d 1109, 1115 (9th Cir. 2013) (quoting *Iqbal*, 556 U.S. at 678). These factual determinations are to be made in the light most favorable to the plaintiff. *Sanders v. Kennedy*, 794 F.2d 478, 481 (9th Cir. 1986). A Rule 12(b)(6) motion to dismiss should therefore be denied "unless it appears beyond doubt that the plaintiff can prove no

set of facts in support of his claim which would entitle him to relief." *Wilhelm v. Rotman*, 680 F.3d 1113, 1121 (9th Cir. 2012). Further, a motion to dismiss should not be granted if material issues of fact are unresolved, *Nelson v. Quimby Island Reclamation Dist. Facilities Corp.*, 491 F. Supp. 1364, 1383 n.44 (N.D. Cal. 1980), or if the motion requires that the court make factual determinations, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1009 (S.D. Cal. 2014). Even doubt as to a plaintiff's ability to prove her case or the remote prospect of a plaintiff's ultimate recovery are not reasons supporting dismissal. *Twombly*, 550 U.S. at 556; *Jurin v. Google, Inc.*, 768 F. Supp. 2d 1064, 1069 (E.D. Cal. 2011).

ARGUMENT

I. Plaintiff Has Article III Standing For All Her Claims.

This Court has already ruled that Plaintiff has alleged facts sufficient to establish Article III standing for her claims. Dkt. 83 at 4 (ruling that Plaintiff had established standing by pleading a claim under the SCA and proceeding to measure each of Plaintiff's claims against the standard set forth in Rule 12(b)(6)). Despite the Court's resolution of this issue, Defendants continue to insist that Plaintiff lacks standing. Dkt. 89 at 7-11. Although they concede, as they must, that the Ninth Circuit's *In re Zynga Privacy Litigation* decision grants Plaintiff standing for her SCA claim, Defendants argue that Plaintiff has not established injury in fact and therefore lacks standing to assert her state-law claims. They are wrong.

To demonstrate Article III standing, "a plaintiff must plead and prove that she has suffered sufficient injury to satisfy the 'case or controversy' requirement of Article III of the United States Constitution." *In re Adobe Sys. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 U.S. Dist. LEXIS 124126, at *17 (N.D. Cal. Sept. 4, 2014). This standard requires a plaintiff to allege: (1) an injury-in-fact that is concrete and particularized, as well as actual or imminent; (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that the injury is redressable by a favorable ruling. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000). At the pleading stage, "general factual allegations of injury resulting from the defendant's conduct may suffice." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Plaintiff's FAC more than meets this standard.

As an initial matter, this Court need not expend judicial resources on an issue it has already resolved and may instead simply adhere to its prior decision that Plaintiff has standing. Although a district judge has discretion to reopen a previously resolved question, such reconsideration is typically appropriate only where the first decision was clearly erroneous; an intervening change in the law has occurred; the evidence on remand is substantially different; other changed circumstances exist; or a manifest injustice would otherwise result. *See United States v. Alexander*, 106 F.3d 874, 876 (9th Cir. 1997); *Thomas v. Bible*, 983 F.2d 152, 155 (9th Cir. 1993). None of these conditions warrant revisiting the question of standing in this case.

But even under the analysis urged by Defendants, Plaintiff still has standing. Her allegations of concrete economic injury – that she did not receive the full privacy protections for which she paid Defendants, allowing them to profit from the sales transaction itself as well as from the market value of her personal information – establish standing for her claims arising under California state law. *See, e.g., In re Linkedin User Privacy Litig,* 932 F. Supp. 2d 1089 (N.D. Cal. 2013) (economic harm based on the "benefit of the bargain" has been recognized as a viable basis for standing); *In re Toyota Motor Corp.*, 790 F. Supp. 2d 1152, 1163-66 (C.D. Cal. 2011) (plaintiffs had standing where they sought recovery for an economic harm they alleged they had suffered); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715 (N.D. Cal. 2011) (a plaintiff who paid fees for defendants' services shows injury in fact when she pleads that defendants, in violation of their own policies, disclosed personal information about its customers); *Doe 1 v. AOL, LLC*, 719 F. Supp. 2d 1102, 1111 (N.D. Cal. 2010) (plaintiffs pleaded injury in fact where defendant's "collection and disclosure of [plaintiffs'] undeniably sensitive information is not something that [plaintiffs] bargained for when they signed up and paid fees for [defendant's] service"); *see also* § II.B *infra* (discussing damages for breach-of-contract claim).

Defendants, relying on *LinkedIn*, contend that Plaintiff has failed to allege the kind of economic injury that would support standing. Dkt. 89 at 9. But *LinkedIn* is inapposite: unlike the plaintiffs in that case, Plaintiff has alleged that she paid Defendants in exchange for their privacy protections, and that they retained a percentage of that payment before remitting the remainder to the App vendor. *See* FAC, ¶¶ 4, 46-49, 71, 114, 117; *see also* ¶¶ 91-92 (alleging that Defendants

issued Plaintiff a receipt for her purchase from Google Play and that her financial statements show Defendants as recipients of her payment); Ex. D (Plaintiff's credit card statement showing purchase). *LinkedIn* does not compel the result Defendants suggest. *See, e.g., In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 715; *AOL*, 719 F. Supp. 2d at 1111.

Moreover, Plaintiff has alleged that Defendants' disclosure of her personal information caused her to lose the sales value of that information, which has quantifiable market worth and which Defendants and App vendors use to make App recommendations, generate personalized search results, and target in-App sales and advertising. *See* FAC, ¶¶ 109-116, 152-159; *see also* § II.B *infra.* These allegations show that Defendants' disclosure deprived Plaintiff of her information's economic value and are sufficient on their own to support Article III standing. *See, e.g., Opperman v. Path, Inc*., No. 13-cv-00453-JST, 2014 U.S. Dist. LEXIS 67225, at *82-83 (N.D. Cal. May 14, 2014) (a plaintiff can establish standing by alleging that the defendant's use of the information deprived the plaintiff of the information's economic value); *see also In re Facebook Privacy Litig.,* __ Fed. App'x __, No. 12-15619, 2014 U.S. App. LEXIS 8679, at *2 (9th Cir. May 8, 2014) (ruling that nearly identical allegations supported the element of damages for breach of contract and thus impliedly finding standing as well).

The FAC establishes that Plaintiff suffered a concrete economic injury – she paid for a service she did not receive and in doing so lost the sales value of her personal information – which is traceable to Defendants' conduct and likely to be redressed by a favorable decision. *See Friends of the Earth*, 528 U.S. at 180-81; *Lujan*, 504 U.S. at 561-62. This Court should deny Defendants' motion to dismiss on standing grounds.

II. Plaintiff Has Stated a Valid Claim For Breach of Contract.

A California plaintiff states a breach of contract claim by establishing a contract, her performance or excuse for nonperformance, the defendant's breach, and resulting damages. *Pyramid Tech., Inc. v. Hartford Cas. Ins. Co.*, 752 F.3d 807, 818 (9th Cir. 2014). This Court ruled that the contract as initially pleaded was inadequate and that Plaintiff had not sufficiently established damages. Dkt. 83 at 6-8. The FAC addresses the issues identified by the Court.

A. The FAC Pleads Facts Establishing a Contract.

The FAC identifies and attaches the contracts in effect at the time of Plaintiff's purchase. *See* FAC, Ex. A (Wallet Terms of Service); Ex. B (Wallet Privacy Policy); Ex. C (Google Privacy Policy). The Terms themselves characterize the contracts as "a legal agreement, between you, Google Inc. and Google Payment Corp. ... that governs your access to and use of Google Wallet." Ex. A at 1. The FAC establishes that, for each separate purchase from Google Play, a buyer must establish a new contract *for that transaction* by assenting to the Wallet Terms then in effect. *See* FAC, ¶¶ 34-35, 38, 42-44, 60-61, 88-89, 140 (explaining that the contract is not complete until a Buyer clicks a button agreeing to the current terms, which Defendants revise over time, and authorizing the transaction, which Buyers are required to do each time they make a purchase). Defendants challenge this description of contract formation as a matter of law, *see* Dkt. 89 at 13, but they do not identify any relevant terms that might contradict Plaintiff's allegations or seriously contest that they require Buyers to click a button agreeing to the Wallet Terms each time they make a purchase. To the extent that Defendants contest the accuracy of Plaintiff's account, at best they raise questions of fact that cannot be decided on a motion to dismiss.[7] *See, e.g., Unicom Sys., Inc. v. Elec. Data Sys., Corp*., NO. CV 04-6716 AHM (RZx), 2005 U.S. Dist. LEXIS 45707, at *25-26 (C.D. Cal. Nov. 1, 2005) (parties' intent regarding the formation of a contract or modification to a contract are normally questions of fact reserved for the jury).

B. The FAC Alleges Damages Sufficient to Support Plaintiff's Breach-of-Contract Claim.

This Court recognized that several damages theories could support Plaintiff's contract claim, including loss of benefit of the bargain and diminution in the economic and proprietary value of her contact information.[8] Dkt. 83 at 7. The FAC pleads both grounds.

---

[7] Defendants also argue in a footnote that Plaintiff provided no additional consideration at the time of her purchase that could support a new contract. However, the FAC is rife with allegations of consideration, which Plaintiff provided both in the form of the percentage Defendants kept from her App purchase price and in the value of her personal information. *See* FAC, ¶¶ 67-68, 71, 90-92, 97-116, 141-143, 147-148, 152-156, 159.

[8] The Court also considered whether Plaintiff could state a claim based on future risk of identity theft and rejected the possibility. Dkt. 83 at 8. Plaintiff acknowledges that the FAC contains no new allegations that support this damages theory and so notes the issue only to preserve it for any potential appeal.

1. Benefit of the Bargain.

Pleading economic harm based on a "benefit of the bargain" theory establishes contract damages. *See, e.g., Aerofund Fin., Inc. v. Top Zip Int'l, Inc.*, No. C 11-00221 PSG, 2011 U.S. Dist. LEXIS 134102, at *6 (N.D. Cal. Nov. 21, 2011); *see also* Dkt. 83 at 7. In her FAC, Plaintiff newly alleges that she did not receive the benefit of her bargain because she provided consideration for Defendants' privacy promises (in the form of her App payment, from which Defendants retained a 30% cut, and by providing her personal information, which has economic market value) but did not receive the protections promised by Defendants. *See, e.g.,* FAC, ¶ 159.

This Court previously identified three concerns with this damages theory, concerns that Defendants reiterate in their Motion. First, the Court ruled that Plaintiff's original Complaint did not show she paid for Defendants' privacy promises or "allege that any portion of [her purchase price] was retained by Defendants rather than being transmitted in full to the vendor." Dkt. 83 at 7; Dkt. 89 at 14 (raising same issue). The FAC clarifies that Defendants retained a 30% cut from Plaintiff's App payment before remitting the remaining 70% to the App Vendor. *See* FAC, ¶¶ 4, 46-49, 71, 114, 117; *see also* ¶¶ 91-92 (Defendants issued Plaintiff a receipt for her purchase from Google Play and her financial statements show Defendants receiving payment); Ex. D (Plaintiff's credit card statement with Defendants' name as a payment recipient). Defendants place great weight on the claim that "GPC does not charge a fee to use the Processing Service as a Buyer," *see* Dkt. 89 at 14, but ignore that the terms elsewhere demand that the Buyer "pay fees and other obligations arising from your use of the Processing Service," *see* Ex. A, § 3.1. At best, Defendants' convoluted characterization of the transaction simply does not reflect common-sense reality; at worst, these terms are ambiguous or contradictory.[9] Ambiguous terms must be construed against Defendants, *see Vedachalam v. Tata Consultancy Servs.*, No. C 06-0963 CW, 2012 U.S. Dist. LEXIS 46429, at *26-27 (N.D. Cal. Apr. 2, 2012), and contradictory terms present questions of fact that cannot be resolved on a motion to dismiss, *see Nat'l Union Fire Ins.*

[9] As Plaintiff noted in her opposition to Defendants' first Motion to Dismiss, Defendants define "Product Purchases," which are treated as distinct from "Products" to be "Services" (capitalized). Dkt. 38 at 9-10.

Co. v. Argonaut Ins. Co., 701 F.2d 95, 97 (9th Cir. 1983).

Second, the Court ruled that Plaintiff's initial Complaint did "not allege facts showing that she entered into a new or different agreement upon purchase of the App that could have given rise to new or additional privacy protections." Dkt. 83 at 7. The FAC clarifies that, for each purchase, a Buyer must enter a new contract. *See* § II.A *supra*; *see also* FAC, ¶¶ 34-35, 38, 42-44, 60-61, 88-89, 140. Six operative sections of the Wallet Terms that Buyers must agree to with each purchase apply to Buyers and not to Customers.[10] A Buyer need not even become a mere Customer; indeed Plaintiff became a Buyer by filling out all the required information at the time of her purchase. FAC, ¶¶ 87-88.

Lastly, the Court concluded, and Defendants argue, that the initial Complaint did not establish damages because it did not allege that what Plaintiff received was worth less than what she bargained for. Dkt. 83 at 7-8; Dkt. 89 at 14. The FAC alleges that "the services Plaintiff and Class members ultimately received in exchange for Defendants' cut of the App purchase price – payment processing, in which their information was unnecessarily divulged to an unaccountable third party – were worth quantifiably less than the services they agreed to accept, payment processing in which the data they communicated to Defendants would only be divulged under circumstances which never occurred." FAC, ¶ 151; *see also* ¶ 86. Moreover Plaintiff alleges that her personal information – which Defendants disclosed together with information about her buying interests and her creditworthiness[11] -- has market value, and when Defendants passed it on, Plaintiff lost the potential sales value of that information. *Id.*, ¶¶ 96-106, 110-116, 157. These allegations are sufficient. *See, e.g., Pac. Shore Props., LLC v. City of Newport Beach*, 730 F.3d 1142, 1170-71 (9th Cir. 2013) (noting that damages may be approximated and justly and reasonably inferred; moreover, in ascertaining damages, defendant should bear the risk of any

[10] §§ 3.2 (Online Card Processing Service); 3.6 (Permissible Payment Transactions); 3.8 (Service Fees); 3.10 (Refunds); Section 4.5 (Transacting with Google Mobile Wallet Service and Google Wallet Virtual OneTime Card); 6 (Limitations on Use of Services).

[11] Buying interests are disclosed by linking her personal information to the purchase. Creditworthiness is disclosed by linking her personal information with the fact that she made a payment with a financial card.

uncertainty produced by its own misconduct); *Posner v. Grunwald-Marx, Inc*., 56 Cal. 2d 169, 187 (1961) (contracting party "is entitled to a reduction in the amount called for by the contract, to compensate for the defects"); *Long Beach Drug Co. v. United Drug Co*., 13 Cal. 2d 158, 174 (1939) ("The fact that the amount of damages may not be susceptible of exact proof or may be uncertain, contingent, or difficult of ascertainment does not bar recovery.").

Defendants summarily assert that the "Court's prior analysis ... still applies," *see* Dkt. 89 at 14, but the FAC's new allegations address both Defendant's challenge and the specific issues this Court identified in its earlier ruling.[12] Their Motion should be denied.

2. Market Value of Plaintiff's Personal Information.

As this Court has recognized, the Ninth Circuit recently explained that allegations "that [plaintiffs] were harmed both by the dissemination of their personal information and by losing the sales value of that information ... are sufficient to show the element of damages for their breach of contract" claim. *In re Facebook Privacy Litig.*, __ Fed. App'x __, No. 12-15619, 2014 U.S. App. LEXIS 8679, at *2 (9th Cir. May 8, 2014) (relying on *Gautier v. Gen. Tel. Co.*, 234 Cal. App. 2d 302 (1965) and *Lazar v. Sup. Ct*., 12 Cal. 4th 631 (1996)). The Court rejected this theory as pleaded in Plaintiff's initial Complaint only because she had not alleged a market for her personal information. Dkt. 83 at 8.

The FAC fills in this gap. It alleges that Plaintiff provided valuable consideration for Defendants' privacy services by giving them her personal information, which is a marketable asset for which companies are willing to pay. FAC, ¶¶ 109-105, 152, 159. This information has great value not only to Defendants, but to App Vendors as well. Defendants use buyer information to generate personal App recommendations and target Google Play search results to consumers most likely to purchase, allowing them to profit from increased App purchases.[13] *Id.*,

[12] Defendants also assert, with no logic or authority, that Plaintiff was required to plead lower prices for the App elsewhere. None of Defendants' contractual obligations depend on what kind of terms might be available somewhere else.

[13] For example, Defendants might use the fact that a particular buyer lives in San Francisco to recommend that the buyer consider purchasing Apps related to San Francisco restaurants or Bay Area public transit options. Similarly, Defendants' search tool might list these options first among a user's search results.

¶¶ 110-116, 153-159. Defendants' business model therefore relies on their ability to collect user information and monetize it; if they did not offer privacy protections, users would be far less likely to hand over their personal information, which would decrease Defendants' profitability. *Id.*, ¶¶ 155-156.

Moreover, this kind of information has value for App Vendors as well. FAC, ¶¶ 105, 112, 115. Vendors are not only able to more precisely target their customers via the Google Play store, they also use personal information to build customer profiles, develop personalized marketing efforts, make in-App sales, and generate in-App advertising. *Id.*, ¶¶ 112-113, 115. By making Plaintiff and the Class's customer data available, Defendants denied them the value of choosing whether to reveal or sell their information to Vendors. These allegations plainly show a market for Plaintiff's personal information, and are consistent with the type of allegations approved by the Ninth Circuit. *See In re Facebook Privacy Litig.*, 2014 U.S. App. LEXIS 8679, at *2.

Defendants contend that Plaintiffs' market theory allegations differ from those approved by the Ninth Circuit in the Facebook litigation, *see* Dkt. 89 at 15, but a comparison of the two complaints reveals they are alike: both allege that plaintiffs paid for defendants' services by providing their personal information, which is of value to defendants (and the third parties who obtained the information) because their business models are predicated on the economic gain they accrue from gathering users' personal information, and that as a result of defendants' disclosures, plaintiffs lost the sales value of their information. *Compare* FAC, ¶¶ 97-116, 152-159 with *In re Facebook Privacy Litig.*, No. C 10-02389 JW, Dkt. 92, First Amended Complaint, ¶¶ 113-122 (articulating similar theory of contract damages). Contrary to Defendants' assertions, the Facebook complaint does not contain specific allegations regarding each plaintiff's attempts to sell his or her personal information, and the Ninth Circuit did not demand this type of showing. The FAC adequately alleges that Plaintiff was deprived of her ability to sell her own information on the market and that both Defendants and App Vendors profit from their access to user information. FAC, ¶¶ 96-106, 110-116, 157. Because the FAC alleges a market for the kind of

personal information disclosed by Defendants, it sufficiently pleads loss of the sales value of that information to satisfy the Ninth Circuit's requirements for establishing contract damages. Defendants' Motion to Dismiss on this theory should be denied.

III. Plaintiff's FAC States a Valid Claim for Breach of the Implied Covenant of Good Faith and Fair Dealing.

Under California law, the implied covenant of good faith and fair dealing "requires each contracting party to refrain from doing anything to injure the right of the other to receive the benefits of the agreement." *Avidity Partners, LLC v. State of Cal.*, 221 Cal. App. 4th 1180, 1204 (2013). While it does not "prohibit a party from doing that which is expressly permitted by an agreement," it does bar "a party vested with discretion from exercising that discretion in a manner that is "contrary to the contract's purposes and the parties' legitimate expectations." *Carma Developers, Inc. v. Marathon Dev. Cal., Inc*., 2 Cal. 4th 342, 347, 373 (1992). A claim for breach may therefore "be made out by allegations that a defendant acted in bad faith to frustrate the agreed common purpose of the contract." Dkt. 83 at 9 (citing *Careau & Co. v. Security Pacific Business Credit, Inc*., 222 Cal. App. 3d 1371, 1395 (1990)).

This Court initially ruled that, although this claim could be fleshed out, it was duplicative of Plaintiff's contract claim because she had not sufficiently pleaded that Defendants acted in bad faith other than by disclosing her personal information (the basis for the breach of contract). Dkt. 83 at 9. In response, the FAC contains new allegations describing Defendants' efforts to frustrate the agreed-upon purpose of the contract, particularly their bad-faith failure to inform consumers that Wallet made their personal information available to third parties (failure to inform is a distinct act from the actual disclosure of that information). *See* FAC, ¶¶ 84-85, 166-169. Defendants argue that these allegations are insufficient to support the type of "conscious or deliberate" act required for bad faith, *see* Dkt. 89 at 20, but ignore that the FAC outlines their knowledge of how Wallet worked and their conscious failure to inform consumers of the fact that personal information would be provided to third parties. FAC, ¶¶ 3, 84 (Defendants had sole control over the contract terms and Wallet payment process); ¶¶ 85, 166-67 (Defendants knew how Wallet functioned and that there was a disparity between the privacy promises consumers

agreed to and those they actually received; nonetheless they did not tell consumers about this disparity). These allegations sufficiently establish a "conscious or deliberate" bad-faith act beyond the disclosure alone. *See Careau*, 222 Cal. App. 3d at 1395; *see also Campbell v. eBay, Inc*., No.: 13-CV-2632 YGR, 2014 U.S. Dist. LEXIS 110806, at *9 (N.D. Cal. Aug. 11, 2014) (denying motion to dismiss implied-covenant claim where plaintiff alleged unfair conduct in the exercise of defendant's discretion under the agreement).

Defendants next maintain that they had no duty to tell consumers about their privacy breaches under the Wallet Terms. Dkt. 89 at 20. But the implied covenant is designed to prevent contracting parties from acting in a manner that is "contrary to the contract's purposes and the parties' legitimate expectations." *Carma Developers*, 2 Cal. 4th at 347. The "agreed common purpose" of the Wallet Terms was private transaction of App purchases; indeed, the contract language Defendants drafted was designed to give consumers the legitimate expectation that their information would not be disclosed. *See* Ex. B at 2; Ex. C at 3-4. By deliberately withholding that the transactions were not private, Defendants frustrated consumers' ability to receive the benefits of the agreement they had bargained for. Because the FAC alleges that Defendants acted in bad faith, contrary to the contract's purpose and the parties' expectations, this Court should deny Defendants' Motion to Dismiss.

IV. Plaintiff Has Stated a Valid Claim Under Section 2702 of the Stored Communications Act ("SCA").

Defendants' argument – that all that is at issue is the disclosure of mere "Contact Information" – downplays the sophistication of the Wallet system. It is true that, initially and for the purposes of merely creating a Google account, Plaintiff provided some information with which Defendants might contact her. Plaintiff's subsequent utilization of Wallet, however, required Plaintiff to provide to Defendants a second, separate set of data – the Packet Contents, with which we are concerned – specifically for processing payments. This data was combined with information depicting Plaintiff's purchase interests and creditworthiness (for instance, that she had a financial card in sufficient good standing to support App transactions).

Defendants, by selectively truncating their references to the statute to avoid raising alarm,[14] propose definitions that do not exist. To lift Defendants' fog the Court has to interpret the SCA. When the SCA was created nearly 30 years ago, Congress noted that the purpose of Section 2702 was to *prohibit* providers from divulging contents of electronic communications to anyone other than the intended recipient. S. Rep. No. 99-541, at 37 (1986). The court's interpretive duty is "to find that interpretation which can most fairly be said to be imbedded in the statute and be most harmonious with its scheme and with the general purposes that Congress manifested." *C.I.R. v. Engle*, 464 U.S. 206, 217 (1984).

The SCA defines the term "content," with respect to any wire, oral, or electronic communication, as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The SCA does not define "record,"[15] but, logically, for purposes of Section 2702, it is information that is *not* content. 18 U.S.C. § 2702(c) states that "A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service *not including the contents of communications*" (emphasis added). Thus, under Section 2702, there is information that is the "the substance, purport, or meaning of that communication," and then there is everything else. All electronically communicated information is either the "content" of the communication or "not content."

Defendants concede that the same information can be "content" or not "content" depending the context, noting that Plaintiff "does not allege, for example, that she sent her Contact Information to Google in the body of an email," and correctly implying that doing so would render the "Contact Information" content. Dkt. 89 at 23.

Ninth Circuit cases confirm that context determines how information is treated. *In re Zynga Privacy Litig.*, 750 F.3d 1098 (9th Cir. 2014) drew from *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003). The *Pharmatrak* defendants were accused of disclosing to their clients, with

[14] Paradoxically, Defendants imply that, had Plaintiff alleged that her credit card number was disclosed, a cause of action would exist despite the fact that the *same* statutory exception to disclosure on which Defendants rely *includes* such information. Dkt. 89 at 5 n.3; 18 U.S.C § 2703(c)(2)(F).

[15] *See* 18 U.S.C. §§ 2510, 2711.

medical information, the "names, addresses, telephone numbers, and email addresses" of persons whom defendants had tracked, via cookies,[16] when they provided the information through online forms. *Id*., 329 F.3d at 15. *Pharmatrak* explicitly held that the Section 2510(8) definition of "content" "encompasses personally identifiable information such as a party's name." *Id.*, 329 F.3d at 19. The *Zynga* court noted that, because the *Pharmatrak* users had communicated with the website by entering their personal medical information – including their names, addresses, telephone numbers, and email addresses – into a form provided by a website, the First Circuit correctly concluded that the defendant was disclosing the contents of a communication. *Zynga*, 750 F.3d at 1107.

Similarly, *Yunker v. Pandora Media, Inc.,* No. 11-cv-03113, 2013 U.S. Dist. LEXIS 42691 (N.D. Cal. Mar. 26, 2013), leading *Zynga's* analysis, declined a defendant's request for an automatic categorization of "a person's zip code, gender, or birthday" as non-content because the plaintiff factually alleged that such information *was* the substance of the electronic communication*:* it was not incidentally-generated to facilitate the transfer of the information, but instead was the content desired to be transferred. *Id.*

The FAC makes new factual allegations that establish that the information at issue here is content. Plaintiff used Defendants' Wallet service to transmit electronic signal Packets from Plaintiff's mobile device to Defendants' servers. FAC, ¶¶ 5-8. The purpose and intent of the transmission was to provide certain information – content – in order to allow the purchase transaction. *Id.*, ¶¶ 5, 9, 204. This is separate from data provided for Google or Wallet account registration information: Defendants do not require a real personal name to register for these products and Google users arbitrarily choose their email addresses. Google or Wallet account registration information is *not* billing information. *Id.*, ¶ 88. Packet Contents here are analogous to data that one would write onto a credit card authorization form and place into an envelope for delivery. Accompanying the Packet Content was routing information that ensured the functional

[16] Indeed, Defendants' Google Privacy Policy, incorporated into the GWPP, is replete with references to how Defendants use cookies to collect and use users' information. FAC Ex. C.

Packet Content got to where it was intended to go and was then reconstituted correctly. *Id.*, ¶¶ 64, 197-204, 207.

In a different context, some Packet Content information Defendants disclosed would not be content – for instance, if it appeared as a return address on the front of an envelope. Here, however, the Packet Contents are information directed to Defendants so that they could process Plaintiff's transaction. Thus, the Packet Contents at issue are not record of the electronic communications, but rather its *substance* – the data Plaintiff sent to Defendants, per Defendants' requirements, for Defendants' subsequent use for a specified purpose under specified conditions. FAC, ¶¶ 205-207. The disclosed Packet Content data in the present case fits squarely within this court's controlling precedent. *See Zynga*, 750 F.3d at 1107.

Defendants contend that the 17-year-old *Jessup-Morgan* decision stands for the proposition that a person's identity, categorically, cannot be "content." *Jessup-Morgan v. AmericaOnline, Inc.*, 20 F. Supp. 1105, 1106-08 (E.D. Mich. 1998). However, the court in *Jessup-Morgan* noted that there was no electronic communication for which the contents were disclosed. *Id.* at 1108. *Jessup-Morgan* is bereft of any relevant analysis.

Defendants also cite the 14-year-old decision in *Hill v. MCI WorldCom Communications, Inc.*, 120 F. Supp. 2d 1194 (S.D. Iowa 2000). The *Hill* court held that information "obtained from the general records [the defendant] maintains on all of its customers in the normal course of its business" did not count as "contents" for purposes of the SCA. *Id*. at 1196. Not only do Defendants fail to assert that the Packet Contents provided by Plaintiff for Wallet payment processing services are kept as "general records," but it is clear that not all Google users have Wallet accounts and indeed, registering for and using Wallet entails the separate and discrete execution of the Wallet Terms. Further, the plaintiff in *Hill* made no allegations that such information did qualify as "content." *Id.* at 1195 n.2 (plaintiff's allegation being merely "The information requested by this unauthorized man included invoice/billing information, parties Plaintiff called, addresses and phone numbers of parties called and other confidential information."). *Hill* is not controlling, instructive, or factually similar to the present case.

Chevron Corp. v. Donziger, 12-MC-80237, 2013 WL 4536808 (N.D. Cal. Aug. 22, 2013), appeal dismissed (Apr. 10, 2014) addressed motions to quash brought by "John Doe" defendants trying to prevent their ISPs from disclosing their identities. *Chevron* held that an electronic communication service provider could only "divulge a record or other information pertaining to a subscriber to or customer of such service" to the extent that the disclosure does not "reveal any more about the underlying contents of communication." *Id.* at 6. The court in *Chevron* illustrated non-content information by reference to free Google and Yahoo! account creation as the *Chevron* movants were merely Google or Yahoo! account users. This is unlike the present case where Plaintiff provided functional billing information to Defendants in the form of a discrete message specifically in exchange for services.

Defendants fail to recognize any distinction between information a user may provide to a service provider, such as Google, merely for password recovery purposes or for the user's name to be indicated in the "From" field in an email header (i.e., for record-keeping) and information provided to a service provider for some functional task, like processing a payment transaction. *See Obodai v. Indeed, Inc.*, No. 13-cv-80027, 2013 WL 1191267 (N.D. Cal. Mar. 21, 2013) (limiting discoverable information to "subscriber information," and not the content of subscribers' electronic communications); *Beluga Shipping GMBH & Co. KS "Beluga Fantastic" v. Suzlon Energy LTD.*, No. 10-cv-80034, 2010 WL 3749279, at *5 (N.D. Cal. Sept. 23, 2010) (merely holding that the actual names of the email account holders provided to Google during the account creation process were producible in response to a civil subpoena).

In *Sams v. Yahoo!, Inc.*, No. 10-cv-5897, 2011 WL 1884633 (N.D. Cal. May 18, 2011) aff'd, 713 F.3d 1175 (9th Cir. 2013), the court found that the plaintiff failed to factually allege that the defendant had disclosed content in response to subpoenaed non-content. *Id.*, 2011 WL 1884633, at *7. Quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), this Court observed that the information slated for disclosure, "e-mail to/from addresses and IP addresses constitute addressing information," would not allow its recipient to determine the substance of the communication, i.e., to "find out the contents of ... messages or know the particular pages on the websites the person viewed."). The present case presents different factual allegations, namely,

that Defendants disclosed both electronic addressing information and functional billing information to App Vendors. FAC, ¶¶ 5, 204-206. These allegations preclude dismissal. *Yunker*, 2013 WL 1282980, at *7.

The discovery crises Defendants predict are fictional. Data which is not the "substance, purport, or meaning" of an electronic communication would still be discoverable under 18 U.S.C. § 2702(c)(6). Law enforcement would still be able to acquire non-content information through the administrative procedures outlined in 18 U.S.C. § 2703(a), (b)(1)(B).

Defendants' cited cases involve address data provided to service providers as "registration information" for record keeping, but never for processing or payment. The context in which information is sent by and obtained from consumers can provide additional information about them, including credit worthiness and purchasing interests. For this reason, what qualifies as "contents," and when it does so, is entitled to the kind of sophisticated analysis reflected in *Yunker* and *Zynga*. As these decisions recognize, context matters. Defendants' motion should be denied.

V. Plaintiff Has Stated a Valid Claim under California's Unfair Competition Law ("UCL").

The UCL is one of the broadest pro-consumer remedial business statutes in the nation. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1266-67 (1992). Defendants urge this Court to limit the UCL's reach by: (1) contesting that Plaintiff suffered economic injury, as the statute requires, *see* Dkt. 89 at 16; and (2) by imposing a reliance requirement where none exists, *see id.* at 17-18. Defendants are wrong on both counts.

A. Plaintiff Has Alleged Economic Injury

While Proposition 64 narrowed the category of persons who could sue under the UCL, it also "plainly preserved standing for those who had had business dealings with a defendant and had lost money or property as a result of the defendant's unfair business practices." *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 321 (Cal. 2011). This Court dismissed Plaintiff's UCL claim because, as originally pleaded, it did not sufficiently allege loss of "money or property." Dkt. 83 at 15-16. But the FAC makes it clear that Defendants retained 30% of Plaintiff's App

purchase price, causing her economic loss sufficient to establish standing under the UCL. FAC, ¶¶ 4, 46-49, 71, 114, 117; *see also* ¶¶ 91-92 (alleging that Defendants issued Plaintiff a receipt for her purchase from Google Play and that her financial statements show Defendants as recipients of her payment); Ex. D (Plaintiff's credit card statement showing that Defendants' name appears as a payment recipient; § II.B *supra* (discussing economic damages in the contract context).

Defendants contend that the App Vendor really paid the 30% fee, not Plaintiff, and so she cannot obtain relief under the UCL because it does not permit disgorgement of profits. Dkt. 89 at 16. To begin with, Defendants' byzantine characterization of Plaintiff's purchase transaction – in which Plaintiff actually gave Defendants money and they then passed on some portion of it to the App Vendor – is inconsistent with the FAC's allegations and at best raises a question of fact that cannot be decided on a motion to dismiss. Moreover, "[t]here are innumerable ways in which economic injury [under the UCL] may be shown. A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *Kwikset*, 51 Cal. 4th at 323. Here, Plaintiff paid for a service she did not receive, Defendants kept a portion of that payment, and then they passed on the value of her information to third parties who accrued economic value from its use. That is sufficient to show loss of money or property and establish standing under the UCL.

B. Plaintiff Need Not Allege Reliance Under Either the Unlawful or Unfair Prongs of the UCL.

Any unlawful, unfair, or fraudulent business practice violates the UCL. Cal. Bus. & Prof. Code § 17200. Because the statute is written in the disjunctive, it is violated when a defendant's act violates any prong. *Davis v. HBC Bank Nevada, N.A.*, 691 F.3d 1152, 1168 (9th Cir. 2012). Although the FAC alleges only unlawful and unfair acts, Defendants attempt to shoehorn Plaintiff's claims into the fraud category so they can import a reliance requirement they contend Plaintiff does not meet. FAC, ¶ 221; Dkt. 89 at 17-19. But this Court has already explained that Plaintiff's claims are properly analyzed under the unlawful and unfair prongs, *see* Dkt. 83 at 16

n.2, and neither theory demands a showing of reliance, *see Olivera v. American Home Mortg. Servicing, Inc.,* 689 F. Supp. 2d 1218, 1224 (N.D. Cal. 2010).

Defendants argue that Plaintiff's unlawful and unfair theories are really premised on misrepresentation, and therefore require reliance anyway. Dkt. 89 at 17-18. But this is a mischaracterization. First, virtually any law – federal, state or municipal, statutory or common law, civil or criminal, regulatory or court-made – can serve as predicate for an unlawful violation. *Smith v. State Farm Mut. Auto. Ins. Co.,* 93 Cal. App. 4th 700, 718 (2001). The FAC alleges that Defendants' disclosures of consumers' personal information are predicates for her unlawful claim because they violate the Stored Communications Act, the public policy embodied in California's Online Privacy Protection Act, and Defendants' own contractual obligations.[17] FAC, ¶¶ 222-224. The question whether Defendants' disclosures violated these predicate laws has nothing to do with the truthfulness of their representations.[18]

Plaintiff's unfair UCL claim does not sound in misrepresentation either. The UCL allows a claim for a business practice that is "unfair" even if not specifically prohibited by law. *Korea Supply Co. v. Lockheed Martin Corp.,* 29 Cal. 4th 1134, 1143 (2003). "An act or practice is unfair if the consumer injury is substantial, is not outweighed by any countervailing benefit to consumers or to competition, and is not an injury the consumers themselves could reasonably have avoided." *Woods v. Google Inc.,* No. 5:11-CV-01263-EJD, 2013 U.S. Dist. LEXIS 51170, at *22 (N.D. Cal. Apr. 9, 2013) (internal quotations and citations omitted).[19] The FAC alleges

[17] To the extent Plaintiff's implied-covenant claim alleges a material omission by Defendants, it may arguably fall closer to the reliance line Defendants push. This Court need not resolve the question, however, because Plaintiff's SCA and contract claims, as well as the Online Privacy Protection Act, plainly do not sound in misrepresentation and provide ample predicate violations for an unlawful-prong claim.

[18] Indeed, Defendants concede that Plaintiff's SCA claim provides a predicate for her UCL unlawful theory that does not require a showing of misrepresentation. Dkt. 89 at 18 n.10. Defendants also concede that California's Online Privacy Protection Act prohibits a commercial website operator from "negligently and materially violating the provisions of its posted privacy policy," *see* Dkt. 18 n.9 (quoting Cal. Bus. & Prof. Code § 22576), which similarly does not require a showing of misrepresentation. And they acknowledge that breach of contract in a consumer class action supports a UCL claim. Dkt. 89 at 18 n.8; *see also Arce v. Kaiser Foundation Health Plan, Inc.,* 181 Cal. App. 4th 471, 489-490 (2010).

[19] Although "the proper definition of 'unfair' conduct against consumers 'is currently in flux' among California courts," *see Davis,* 691 F.3d at 1169, no definition demands a reliance showing.

that Defendants' disclosure of personal information in of itself caused consumers substantial injury that they could not have anticipated and that is not justified by any countervailing benefit. FAC, ¶¶ 225-229. Again, whether the disclosure itself caused harm has nothing to do with the veracity of Defendants' representations.

VI. Plaintiff's § 2701 Claim is Repleaded Solely For Purposes of Preserving Appeal and Should Not Be Stricken.

Lastly, Defendants move to strike Plaintiff's repleaded § 2701 claim on the theory that it "exceed[s] the scope of [the] court's leave to amend." Dkt. 89 at 25. The Court should deny this request: the FAC expressly recognizes that this claim was dismissed with prejudice and is included only to preserve any potential appeal. FAC, ¶ 172. While Defendants correctly note that the Ninth Circuit has recently retreated from its previous holdings finding waiver of appeal where plaintiffs failed to replead claims dismissed with prejudice, the authority they cite in no way *requires* that such claims be stricken. *See, e.g., Lacey v. Maricopa County,* 693 F.3d 896, 928 (9th Cir. 2012) (holding that "[f]or claims dismissed with prejudice and without leave to amend, we will not require that they be repled in a subsequent amended complaint to preserve them for appeal" and cautioning that voluntarily dismissed claims would still be "waived if not repled"); *Lamumba Corp. v. City of Oakland*, No. C 05-2712 MHP, 2006 U.S. Dist. LEXIS 82193, at *10-11, 16 (N.D. Cal. Oct. 30, 2006) (declining to strike plaintiff's allegations since even where new allegations "[e]xceed[ed] the scope of a court's leave to amend," there were "not necessarily sufficient grounds for striking a pleading"). The repleaded § 2701 count is not "wholly specious" nor do Defendants even try to argue it prejudices them; indeed, they cannot, since it is included solely to protect Plaintiff's right of appeal and is not an attempt to reassert a claim that this Court has already dismissed. *See, e.g., Sapiro v. Encompass Ins*., 221 F.R.D. 513, 518 (N.D. Cal. 2004) (declining to strike new allegations where they were not wholly specious and defendants were not prejudiced); *Samuel v. Rose's Stores, Inc*., 907 F. Supp. 159, 162 (E.D. Va. 1995) (declining to strike amended complaint where no new causes of action were alleged and defendant did not argue prejudice). The motion to strike should be denied. *See Lamumba Corp.*, 2006 U.S. Dist. LEXIS 82193, at *6 (such motions are "generally disfavored").

CONCLUSION

For the foregoing reasons, Defendants' Motion should be denied.

Respectfully submitted,

/s/ Elizabeth Roberson-Young
Elizabeth Roberson-Young

Kathryn Diemer
Diemer, Whitman & Cardosi, LLP
75 East Santa Clara Street, Suite 290
San Jose, CA 95113
Phone: 408-971-6270
Fax: 408-971-6271
kdiemer@diemerwhitman.com
CA Bar No.: 133977

Frank Jablonski
Progressive Law Group, LLC
354 W. Main Street
Madison, Wisconsin 53703
Phone: 608-258-8511
Fax: 608-442-9494
frankj@progressivelaw.com

Mark Anthony Bulgarelli
Elizabeth Roberson-Young
Progressive Law Group, LLC
One N. LaSalle Street, Ste. 2255
Chicago, Illinois 60602
Phone: 312-787-2717
Fax: 888-574-9038
markb@progressivelaw.com
liza@progressivelaw.com

Counsel for Plaintiff Alice C. Svenson

CERTIFICATE OF SERVICE

I, Elizabeth Roberson-Young, am a resident of the State of Illinois and over the age of eighteen years. My business address is 1 N. LaSalle Street, Chicago, IL 60602. On September 30, 2014, I served Plaintiff's Opposition to Defendants' Motion to Dismiss electronically with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record for all parties that have appeared in this proceeding.

I declare under penalty of perjury under the laws of the United States that the above is true and correct.

Executed on September 30, 2014, at Chicago, Illinois.

/s/ Elizabeth Roberson-Young
Elizabeth Roberson-Young